ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРІЄМСТВА

***Сметанов М.В.**, магістр, Харківський національний університет міського господарства імені О. М. Бекетова*

Будь-яке знання є сила. А що таке знання? Це інформація. І недарма кажуть «Той, хто володіє інформацією,той володіє світом». Зараз інформація може бути як засобом забезпечення безпеки, так, у свою чергу, і загрозою та небезпекою.

Наданий момент установлюється інформаційне суспільство. Це має як свої плюси так і мінуси. Зокрема з одного боку, пришвидшилася передача інформації значного обсягу, прискорилась її обробка та впровадження. З іншого – серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо. Актуальність забезпечення інформаційної безпеки зумовлена впровадженням новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя і в діяльність органів державної влади.

Тривалий час розуміння інформаційної безпеки в наукових та нормативно-правових джерелах ототожнювалося тільки з захистом інформації, що значно звужувало її сутність. Саме тому, з низки питань, присвячених розгляду проблеми забезпечення інформаційної безпеки, найбільш вивченими та дослідженими її аспектами є безпека інформації.

Але до інформаційної безпеки підприємства не слід відносити лише захист інформації, адже безпека має набагато ширше значення ніж охорона чи захист.

Зокрема важливою складовою інформаційної безпеки підприємства є інформаційно-аналітична робота. Основним завданням якої є збирання всіх видів інформації, яка може мати в плив на суб’єкт господарювання:

- про економічний стан фірми, регіону, своєї країни, країн, в яких є партнери і т.д.;
- про політичну ситуацію в регіоні і країні; про морально-психологічний клімат в колективі;
- про конкурентів і методи конкуренції (добросовісною і недобросовісною);
- про кримінальні структури і можливі терористичні погрози;
- постановка завдань по перевірці потенційних партнерів, клієнтів, конкурентів;
- розробка програм протидії промисловому шпигунству, терористичним погрозам і іншим методам недобросовісної конкуренції;

- розробка програм дезінформації конкурентів:
- через засоби масової інформації;
- через інформаційно-телекомунікаційні канали;
- через постачальників, суміжників, партнерів, клієнтів;
- шляхом організації псевдопросочування конфіденційної інформації;
- розробка програм захисту конфіденційної інформації.
- а також аналіз цієї інформації, прогнозування подальшого розвитку подій.

Обробка інформації інформаційно-аналітичним відділом:

Першою і найважливішою операцією є аналіз, який служить додатковим фільтром, що відкидає непотрібне і що є захистом від шуму без підстави. Ця операція полягає перш за все у визначенні важливості, точності і значущості інформації. Інформація є важливою, якщо вона зв'язана, тобто має зв'язок з елементами бази, і якщо вона здатна внести внесок до організації. Коли внесок значимий і безпосередній, інформація вимагає термінових дій.

Інформація, що не має значення, повинна бути виключена щоб уникнути втрати часу і енергії. Не завжди легко встановити, є інформація достовірною або помилковою, особливо якщо вона містить відомості про події, які ще не відбулися.

Допускається два критерії, по яких можна судити про точність інформації, надійність джерела і самої інформації. Головним критерієм правдоподібності є пошук підтвердження за іншими джерелами, якщо можливо - за незалежним.

Серед сучасних підприємців Заходу панує думка, що, використовуючи всього п'ять основних правил безпеки, можна добитися значних успіхів в бізнесі. До них відносять:

1.) розвідку;

2.) професіоналізм у встановленні контактів - мінімальні витрати часу і сил для пошуку інформації, необхідної для налагодження контакту;

3.) кваліфікацію менеджера - витрати часу тільки на потрібних людей;

4.) уміння долати перешкоди, пошук варіантів і обхідних шляхів для дозволу виникаючих проблем;

5.) уміння завершувати операцію, нехай навіть з негативним результатом - це все ж краще, ніж відсутність якого-небудь результату.

Іншою, і не менш важливою складовою інформаційної безпеки є збереження інформації.

Існує декілька способів збереження важливої інформації:

- усний – тобто запам’ятати інформацію. Є малоефективним, так як людина не може запам’ятати великий об’єм інформації, а також нам властиво її забувати.
- на папері (письмовий) – є дуже важливим, адже на даний час усі документи складаються і записуються на папері. Термін зберігання тривалий, але велика кількість інформації займає багато місця, і для довготривалого збереження необхідні сприятливі умови. Інформація є мало захищеною, і

якщо її велика кількість, то з нею важче працювати, затрачаючи велику кількість часу.

- електронний – збереження інформації на цифрових носіях, комп'ютерах, ком пакт дисках. Є найзручнішим і найсучаснішим. Дозволяє зберігати велику кількість інформації при цьому займаючи якомога менше місця, проте і він має свої мінуси. Наприклад, якщо комп'ютер підключений до мережі Інтернет чи до іншої локальної сітки, до за допомогою шпигунських програм можливо легко добути з нього будь-яку інформацію, і не має значення скільки рівнів захисту він має.

Проте жодний з цих методів не є досконалим, і як би ми її не зберігали, в житті є завжди місце випадку.

Проблема захисту інформації: надійне забезпечення її збереження і встановлення статусу використовування - є однією з найважливіших проблем сучасності.

Цілями інформаційної безпеки підприємства є:

- запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації;
- запобігання погрозам безпеці особи, підприємства, суспільства, держави;
- запобігання несанкціонованим діям із знищення, модифікації, спотворення, копіювання, блокування інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси і системи, забезпечення правового режиму документованої інформації як об'єкту власності;
- захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, наявних в інформаційних системах;
- збереження, конфіденційності документованої інформації відповідно до законодавства.

Причини втрати і пошкодження інформації можуть бути різними. Найчастіше це зараження вірусами. Сьогодні нікого не здивуєш існуванням комп'ютерних вірусів.

Окрім програм, які займаються псуванням, знищенням даних, псуванням апаратного забезпечення, уповільненням роботи комп'ютера, існують віруси, які стараються нічим не видати своєї присутності, а потихеньку збирають інформацію, наприклад, паролі, ведуть контроль за натисненням клавіш користувача ПЕВМ, а потім передають знайдену інформацію на заздалегідь певну адресу, або здійснюють які-небудь певні дії. Ці віруси відносяться до так званих «троянських коней».

На сьогоднішній день найменш контрольована область – це інформація, що надсилається за допомогою електронної пошти. Цим активно користуються інсайдери і несумлінні працівники, і левова частка конфіденційної або небажаної інформації витікає саме через Інтернет, за допомогою повідомлень електронної пошти.

Важливим елементом організації інформаційної безпеки є поділ заходів на групи. У теорії та практиці виділяють такі три групи: активні засоби

захисту (наприклад, розвідка, дезінформація, зашумлення тощо); пасивні (охоронні) засоби (наприклад, встановлення екранів проти несанкціонованого витоку інформації тощо); комплекс засобів підтримки - органічне поєднання попередньо вказаних груп щодо моделювання потенційних (невідомих раніше практиці) загроз.

Таким чином, на сьогоднішній день пропонується безліч способів забезпечення безпеки інформації, але не всі вони є ефективними. Відомо, що тільки «комплексна система може гарантувати досягнення максимальної ефективності захисту інформації, оскільки системність забезпечує необхідні складові захисту і встановлює між ними логічний і технологічний зв'язок, а комплексність, що вимагає повноти цих складових, всеосяжності захисту, забезпечує її надійність»

Особливість безпеки інформаційної діяльності підприємства полягає у запобіганні, протидії та подоланні природних (стихійних), техногенних і людських загроз, здатних порушити (чи припинити) діяльність підприємства.